Coping with U.S. Regulation of International Conduct: Compliance Strategies for the Foreign Corrupt Practices Act

Gregory Husisian
Foley & Lardner LLP
3000 K Street, NW, Suite 600
Washington, DC 20037-5143
202.945.6149
ghusisian@foley.com

November 2009

©2010 Gregory Husisian, of Foley & Lardner LLP

Coping with U.S. Regulation of International Conduct: Compliance Strategies for the Foreign Corrupt Practices Act

In recent years, the U.S. Government has become increasingly aggressive in enforcing U.S. laws designed to regulate the conduct of U.S. citizens and companies operating abroad. As a result, multinational firms face multiplying compliance concerns, especially with regard to the Foreign Corrupt Practices Act, export control and sanction regulations, the anti-boycott law, and anti-money laundering requirements. In the first of three articles, the author presents compliance strategies for corporations attempting to manage the risks posed by the Foreign Corrupt Practices Act.

GREGORY HUSISIAN
FOLEY & LARDNER LLP

INTRODUCTION

Just past its 30th birthday, the Foreign Corrupt Practices Act of 1977[1] today poses the greatest liability risks ever for U.S. firms and other covered entities pursuing business opportunities abroad. This increased risk arises due to the increased chance of prosecution by the U.S. government, the government's increased appetite for large fines, and the increased risk of multiple prosecutions due to other countries having adopted FCPA-equivalent laws, as perhaps best symbolized by Siemens being forced to pay $1.6 billion in fines to anti-corruption authorities in Europe and the United States.

Most U.S. entities by now are familiar with the FCPA, which in general terms prohibits U.S. individuals and U.S. companies, or people or entities acting on their behalf, from "corruptly" making a payment or giving "anything of value" to a foreign official (or to any other person while "knowing" that it will be used for a corrupt payment) for the purpose of influencing the foreign official to use his position to

[1] Pub. L. No. 95-213, 91 Stat. 1494 (codified at 15 U.S.C. §§ 78dd-1 and 78dd-2, as amended). The Act has been amended twice, once as part of an omnibus trade bill passed in 1988, *see* Omnibus Trade and Competitiveness Act of 1988, Foreign Corrupt Practices Act Amendments, Pub. L. No. 100-418, tit. V, subtit. A, pt. 1, §§ 5001-5003, 102 Stat. 1107 *et seq.* (1988 amendments), and once to implement the changes required when the United States implemented the Organization of Economic Development's anti-corruption initiative. *See* International Anti-Bribery and Fair Competition Act of 1998, Pub. L. No. 105-366.

©2010 Gregory Husisian, of Foley & Lardner LLP

help obtain or retain business or to secure an "improper advantage."[2] But while the broad dictates of the law are clear, less apparent are steps that companies can take to comply with the law.

ESTABLISHING AND IMPLEMENTING AN EFFECTIVE COMPLIANCE PROGRAM

Some companies only grudgingly implement compliance programs, viewing them as an impediment to conducting business. But a corporation needs to have a firm grip on how its funds are being disbursed and to have assurances that its corporate interests—including its interest in avoiding crimes that can result in adverse publicity and huge fines—are being implemented, even by employees or intermediaries operating far from corporate headquarters. Viewed in this way, a compliance program is an extension of the kind of risk and asset management that corporations already are imposing as part of their internal control procedures.

Establishing a Program: General Principles

A good FCPA compliance program serves four complementary purposes:
(1) educating employees about anti-bribery and recordkeeping requirements;
(2) effectively communicating that the company is serious about its anti-bribery initiatives, and that they are not just window dressing to be discarded when they get in the way of an important sale; (3) providing a means by which employees can distinguish between clear-cut areas where few FCPA concerns are present and those where involvement of experts is necessary; and (4) providing a means of monitoring adherence to policies and encouraging the early reporting of problems so that the company can take ameliorative action.

A company needs to tailor the amount of resources it devotes to a compliance program to its own business risks and needs. A useful place to start is to consider procedures that are appropriate for companies that have substantial operations in multiple foreign countries, operate in industries where the risk of violations is higher (such as defense, energy, or other industries with multiple recent enforcement actions), or countries with a reputation for corruption. These types of high-risk companies need to devote substantial resources to compliance, while companies that are at lesser risk would have the option of implementing scaled-down procedures.

Regulators expect that companies that fall in the high-risk category, in particular, will respect certain principles in the formation of compliance programs. They expect that these companies will:

---

[2] *See* 15 U.S.C. §§ 78dd-1 (issuers), 78dd-2 (domestic concerns).

©2010 Gregory Husisian, of Foley & Lardner LLP

- Apply a uniform standard across the company for all divisions and countries of operation. While it can be tempting to relax standards when operating in a country that is more freewheeling, doing so communicates a message that anti-bribery requirements are a hurdle for employees to skirt as closely as possible. Additional problems arise when employees move from one country or division to another and unnecessarily confront differing standards.
- Promulgate a clear policy that takes away decision-making in "gray areas" from employees who are not experts in the FCPA to people, either at corporate headquarters or in the general counsel's office, who are well versed in the law.
- Provide comprehensive training to new hires with regular supplemental training (with more intensive training for key employees, such as those in sales and marketing, those who operate abroad, finance employees, and people who supervise same).
- Prepare a written compliance policy that includes both a recitation of the law and real-world examples that are relevant to the industry and business.
- Prepare procedures in advance for dealing with foreign agents, distributors, and joint venture partners, including model FCPA provisions and procedures for performing due diligence that can be tailored to meet individual situations as they arise.
- Establish procedures to ensure tight control over the distribution and tracking of expenditures.
- Develop procedures to ensure the retention of all due diligence and FCPA compliance actions.
- Set up a structure for deciding whether a potential FCPA violation exists by people who are independent of the transaction and who have no pressure to approve suspect transactions.
- Establish procedures for the confidential reporting of suspected problems.
- Establish procedures to evaluate potential FCPA violations and to investigate them.

In putting these requirements into practice, a company will need to tailor the program to its industry and needs. A good program will:

- Contain elements to show that the company is establishing a culture of compliance.
- Be accessible and written in plain English.
- Allocate senior-level responsibility at both the management and director levels.

- Have procedures governing the training and monitoring of employees.
- Ensure that third parties are subjected to adequate due diligence.
- Contain provisions to allow the reporting of problems, including anonymous whistle blowing.
- Make clear that the company will severely discipline violators of the policy.

Responsible officials must have the authority to implement the program and to use company resources to monitor, audit, and test the compliance procedures to ensure that they are faithfully implemented. Regulators expect that the company will regularly update the policy to incorporate new lessons as the company encounters and resolves problems and as the DOJ and SEC announce new enforcement actions that provide guidance regarding FCPA compliance norms.

The involvement of senior management does not end once the program is implemented. The goal is to foster a corporate culture where compliance is viewed as part of the corporate mission rather than a barrier to completing transactions. Employee performance reviews should place some weight on an employee's adherence to compliance standards. Most programs have procedures for employees to report compliance concerns that are independent of normal business channels so the employee knows he can share concerns without fear of retribution. Many companies also choose to establish procedures for the vetting of third-party relationships, including through the performance of systematic due diligence that is reviewed by people who are not directly associated with the completion of the transaction.

Implementing a Program

Even the best program, if not properly implemented, will be ineffective. Proper implementation of a program depends on establishing from the outset that the firm has a culture of compliance and that it will not countenance short-term profit gains at the expense of an increased risk of an FCPA violation. Communication of this message is best served by including business people within the presentation of the FCPA policy. Too often firms turn over implementation of the FCPA policy to the lawyers, which makes it seem like there is a tension between the compliance program and the firm's business objectives. Further, the company should not implement the program purely as a top-down initiative and instead should involve appropriate division people. It is best if presentations of the program involve local business people who are aware of the situation on the ground and can offer practical advice on how to implement the program.

Typical Steps in Designing a Program. A proper program cannot be designed in a vacuum. Regulators stress that a compliance program should reflect the individual company's requirements, including its own procedures for tracking payments, its specific corporate organization, and its business interests. The following general considerations form the core of the design of the program:

- ***Risk Identification.*** The first step is to consider the risks posed by the company's business activities. This includes an evaluation of where the company does business, its particular product line, and the company's history of compliance issues. Regulators stress that companies should consider not just the company's FCPA risk profile, but also whether it has run into trouble in other areas, including for export control or import violations, which could indicate a careless corporate culture toward compliance issues. Companies also should carefully consider the degree of interaction with foreign government officials.
- ***Control Identification.*** The next step is to determine what controls have already been established and to evaluate their adequacy and defects. Auditor letters, such as SAS 30 warnings from accountants, should be considered, but regulators have publicly stated that a more far-reaching inquiry than is required by accounting-driven evaluations should take place.
- ***Resource Identification.*** The controls the company implements must be commensurate with the resources available. A company should not, for example, put in place a program that demands substantial due diligence of every foreign agent hired if it has not made the decision to fund such activities. Otherwise, it risks setting itself up to look like it has failed to meet its own compliance standards. Once the risk and necessary controls have been identified, a company can develop a realistic sense of the cost of a program and the resources needed to run it.
- ***Scope and Objectives Identification.*** The next step is to evaluate the scope and objective of the program: who needs to be covered; what level of training is required; what monitoring needs to occur, and so forth. Many companies will vary the level of training and oversight based upon the person at issue and his responsibilities. It is a good idea to consider the level of oversight, and what liaisons it wants at the director and management level, as well.
- ***Compliance Procedures.*** Most companies prefer to implement FCPA controls on a company-wide basis, including with regard to how payments and disbursements are to be controlled. Companies often create models for typical situations, including hiring agents, setting up joint ventures, hiring distributors, and conducting due diligence. It is advantageous to have procedures in place for dealing with red flags as they arise, so that potential violations are both unearthed and investigated in a prompt fashion.
- ***Accounting Procedures.*** In evaluating compliance procedures, companies generally implement both compliance procedures and internal accounting controls simultaneously. The two naturally work together, with the accounting controls being a useful tool to ferret out substantive violations of the FCPA. An effective set of accounting controls is the final step in ensuring that illegal payments are not made and they

should incorporate review and approval guidelines designed to detect and deter questionable payments.

- ***Testing Procedures.*** It is difficult to have a strong compliance program unless it is regularly tested, probed, and analyzed. Many companies now monitor all procedures after the fact, including by ensuring that all contracts for distribution agreements, joint ventures, and consultants have included FCPA clauses. Where necessary, regular annual certifications need to be signed by key employees and third parties. Companies often will monitor due diligence procedures to ensure that the company is regularly following them.
- ***Reporting Procedures.*** Reporting procedures are a key element of any FCPA compliance program. Companies should have clear procedures in place from the start regarding when the compliance officer will take care of things, when the general counsel's office will get involved, and when senior management and directors will be informed. The Sarbanes-Oxley financial control reporting requirements also indirectly come into play when companies are deciding how involved senior management should be and when apparent FCPA failures arouse suspicions that a company's internal controls are not adequate to meet required corporate standards.
- ***Updating Procedures.*** Finally, the days of putting a compliance program in place and then leaving it unattended are long gone. With the increasing number of SEC and DOJ investigations, state of the art is a constantly moving target. Regulators expect that the general counsel's office or the person in charge of compliance will regularly monitor developments in the field and incorporate them into an updated program that will reflect the latest thinking on FCPA enforcement and compliance.

Typical Elements of a Compliance Program. As noted above, the DOJ and the SEC have little patience with one-size-fits-all FCPA compliance programs. Since most companies have moved beyond these cookie-cutter programs to more sophisticated programs that are tailored to the business environment of the particular company, the DOJ and SEC are unlikely to view generic programs very favorably should a problem arise. Still, all successful programs share certain elements, which typically include:

- ***A Written Policy Statement.*** A policy statement is a statement from the head of the company that succinctly sets out the company's commitment to comply with all anti-corruption laws and regulations. It should be more specific than the general code of conduct statements that many companies use that promise just general adherence to the law. The policy statement should be written in straightforward, plain language. It also should stress the importance of timely and accurate accounting for all payments, regardless of purpose.
- ***A Manual of Business Ethics and Procedures.*** A business manual generally will include not only a complete copy of the company's

policies, but also real-world examples of some of the tricky situations that can arise, such as payments for travel and lodging, dealing with foreign officials, company policy on facilitating payments, and so forth. The manual should present detailed information about reporting, company procedures for approving payments, standards for entertainment of government officials, and sample forms for proper accounting for expenditures. A growing trend is for companies to provide links on their intranet to local laws that also govern the payment of bribes to government officials (and necessarily vary from country to country).

- ***Education and Training Programs.*** A good education and training program has both a written and a presentation component. The program is enhanced by drawing on real-world examples, such as case studies drawn from actual problems confronted by the company in the past. Training should be considered for both new employees and annually for long-time employees. Many companies use a mix of on-line training and in-person training, with the latter (and more expensive) option tending to be reserved for employees who operate in high-risk areas or who have frequent interactions with government officials. The company should maintain an attendance log and have all employees sign acknowledgment forms showing that they have reviewed the compliance materials and understand their responsibilities to comply with the company's program.
- ***A Methodology for Tracking Payments Accurately.*** A system for employees to turn in all receipts, and to keep track of all disbursements and the nature of the transaction, is part of any compliance program. The goal is to allow the timely and accurate recording of all disbursements. Although the FCPA only imposes this requirement for issuers (*i.e.*, public companies that are registered under the 1934 Securities and Exchange Act), all companies operating internationally should consider having a similar system in place since it is difficult to identify potentially illegal payments without proper tracking of disbursements.
- ***Coverage of Common Issues.*** Many common situations can be anticipated from the outset and procedures set up in advance to deal with them. Typical issues that are covered by compliance programs include setting policies on facilitating payments to foreign officials, policies regarding payment of promotional or marketing expenses involving foreign officials (including regarding gifts, meal, travel, and entertainment), and procedures for political contributions. Standardized provisions can be developed for common third-party situations, including FCPA provisions regarding agents, joint ventures, and distributors.
- ***A System of Reporting Suspected Violations.*** Most companies either set up a compliance committee or have a senior individual who is

responsible for coordinating all anti-bribery initiatives. Independent responsibility is essential because people who are involved in business-generating activities could be placed in a situation where their judgment as to whether to proceed is colored by business issues. If the compliance officer is not the general counsel, the company should establish procedures for regular coordination with the company's legal department. Although the precise elements of the reporting system will vary depending upon how the company and the program are structured, common elements are reporting hotlines and procedures for the anonymous reporting in writing of suspected violations.

- ***Top Management Access.*** Thought should be given at the outset regarding the means of communicating with management. Some companies take care of this by having the general counsel oversee compliance, which should give easy access to top management due to regular contact of the general counsel with high-level officers. Other companies will use a structure in which the compliance officer is a direct report of the president or CEO of the company.
- ***A System of Discipline.*** Finally, a company should develop procedures to address violations of the FCPA. Coverage should be both for direct involvement in the scheme and for failure to prevent and detect misconduct by others.

Companies increasingly are considering implementing a mechanism for the periodic check of compliance; otherwise, standards tend to slip and there is no mechanism to revisit problems that are not initially noticed. An internal audit and compliance review, if implemented, should evaluate company and employee compliance and identify procedures that the company needs to modify or strengthen.

Many companies undertake top-to-bottom reviews of their policies every three to five years by either an independent legal or auditing firm. Testing of FCPA controls differs from testing of other compliance areas in that it involves careful risk assessment as a means of focusing inquiry. While it is not possible to test every transaction in evaluating the rigor of the program, companies can focus on areas of highest risk and work backwards. Auditors will focus on areas where the most money is generated or where corruption risk is highest (based upon business or country-of-operation factors) as areas of special interest. Auditors generally then will focus on areas of the most common violations, including expense reports, overpayments to vendors, credit invoices, payments to distributors, travel expenses and reimbursements, and any direct payments to government officials, however classified.

Anticipating Problems: Setting the Stage for Internal Investigations

An additional issue that companies need to anticipate in any compliance program is how it will conduct internal investigations. No matter how strong a firm's compliance program, at some point the company will need to conduct some kind of internal investigation. Thus, a proper compliance program will have established procedures in place for deciding when and how the company will conduct an internal investigation.

Most companies use a tiered-investigation strategy, progressing based upon the level of alarm raised by the facts. Usually companies start with local investigation, often directed by someone who is designated as an investigator at the regional or headquarters level, with the basic goal of determining whether there is a real issue. If facts appear to warrant further inquiry, the general counsel's office should become more involved to ensure proper protection of evidence and involvement of people who can appreciate the subtleties of evidentiary and FCPA points. The general counsel also can determine whether facts appear serious enough to report to senior management. Consideration, too, needs to be given as to whether the audit committee needs to be informed, which certainly needs to occur if the violation appears to be one that draws the corporation's internal controls into doubt. The next step—and it is a quantum leap in terms of intensity—is to consider the hiring of outsiders to conduct a full-blown investigation. Outside counsel and forensic experts can delve into records and conduct an exhaustive investigation. The final and most dreaded step is to consider reporting to the DOJ and the SEC.

A question that always arises is how to determine what scenarios a company should investigate. The easy advice is: investigate everything. But as desirable as this would be from a pure FCPA perspective, it ignores the fact that companies can receive a large number of tips and innuendo that in the end turn out to be meaningless noise. Companies need to assess credibility at the outset to determine which tips merit serious follow up and commitment of a substantial amount of resources, and which receive lower priority.

Most companies that operate in multiple jurisdictions have a pretty good idea of which business units are most likely to be flashpoints. Some companies that operate worldwide have set up matrices to help inform the decision as to whether to investigate. This can be important, since it helps focus the company from the beginning in its thoughts about which areas of the company are most likely to lead to FCPA problems. This thinking can then carry over to the decision as to whether an investigation should be ramped up. Events or tips that might seem innocuous in certain areas of the world can appear much more ominous when a business unit that has frequent government contact, or that operates in a country that ranks high on rankings of corruption, is at issue.

Anticipating Serious Investigations

Companies should give thought at the outset regarding when to involve senior management and the audit committee. Of all the topics to be covered, this one is the hardest to provide parameters for ahead of time. Obviously, senior management should be told when there are glimmers that the problem is serious and widespread, and should not (or should be told only in summary form as part of periodic reports) when there are not. Most problems fall in between, making it difficult to tell what to do.

Centralization of reporting helps take care of this problem. The general counsel or the chief ethics officer should decide, not local employees. This ensures that someone with a feel for the sensibilities of U.S. law is consistently making the judgment call.

Companies also should give thought regarding when to involve outsiders. No real guidelines can be set up in advance for when outside counsel should be brought in. This really is a you-know-it-when-you-see-it area. For most companies, the trigger point is when it appears that an FCPA issue is part of a larger pattern, involves a lot of money, involves a number of employees, or has been going on for a long time. If it appears that there is a systemic problem, and that the potential FCPA issues permeate a certain division or region, or even the company itself, then most companies will opt to bring in outsiders to ferret out the problems. At that point, intrusiveness and cost are outweighed by the need to get the universe of problems out into the open.

An internal investigation necessarily covers a lot of ground. A company will need to consider a host of issues, including: how to determine if allegations of potential violations are credible; what steps need to be taken to preserve documents (both paper and electronic); how to evaluate the risks of potential third-party disclosure; how to get to and interview relevant witnesses; how to determine if there are any disclosure obligations; and other issues relating to the how and what of an investigation. A company should consider these procedures at the outset so that they do not have to be made up on the fly.

The Perennial Problem of Agents and Distributors

Because agents and distributors are used so often by many companies, no compliance program can function unless it successfully deals with these intermediaries. The DOJ and the SEC look askance at attempts to place agents outside the confines of a company's FCPA compliance responsibilities. For example, in *In the Matter of Oil States Int'l, Inc.*,[3] a key point in the SEC charge was that the subsidiary of an issuer hired a consultant without providing any formal training or education to the consultant. Even more ominously, in its 2007 complaint charging Baker Hughes Inc. with violations of the FCPA, the SEC relied on a theory that the knowledge requirement was satisfied where the "company failed to adequately assure itself that such payments were not being passed on" to a foreign official.[4]

[3] *See* Thomson West, 5 The FCPA Reporter 699.9504 (2006 ed).

[4] *See* SEC v. Baker Hughes Inc. and Roy Fearnley, Complaint H-07-1408 (Apr. 26, 2007) at ¶ 7. This formulation was repeated numerous times. *See, e.g.*, *id.* ¶ 6 (alleging a section 30(A)

©2010 Gregory Husisian, of Foley & Lardner LLP

This standard of failure to inquire, while at odds with the amendment of the knowledge standard in 1988 to eliminate liability where there was only a "reason to know" of a corrupt payment,[5] nonetheless raises the stakes whenever an intermediary is employed.

Due Diligence. How much due diligence to conduct prior to the retention of an intermediary is an issue that many companies have trouble deciding. The degree of due diligence that is prudent depends on numerous factors, including the dollar value of the arrangement, the expected contact with government officials, and the country at issue.

Part of due diligence is to check that the agent or distributor being hired is up to the task. This does not just serve a business purpose. An intermediary that seems to be running a real business is less likely to be a front that only can operate due to illegitimate contacts within the foreign government. Any agent or distributor hired should demonstrate that it has a good understanding of local business practices, adequate capital and resources necessary to finish the job contemplated, adequate facilities for operation, and financial resources commensurate with the responsibility being trusted to it.

There are three basic goals for any due diligence inquiry: (1) to weed out, to the extent possible, people or firms who are likely to make bribes (or to be otherwise unsuitable for the job contemplated); (2) to document how hiring decisions were made, and why; and (3) to establish that, in the event a violation later occurs, there was no way that the hiring firm could have known about it because the agent or distributor was carefully vetted.

---

violation for an Angolan official where the company "failed to make an adequate inquiry"); *id.* (same for Nigeria, where "the company failed to adequately assure itself that such payments were not being passed on, in part, to Nigerian Customs officials); *id.* (same for agent who worked in Kazakhstan, Russia, and Uzbekistan "under circumstances in which the company failed to determine whether such payments were, in part, to be funneled to government officials in violation of the FCPA").

[5] The DOJ and the SEC interpret the knowledge requirement as encompassing any situation where a company has failed to conduct sufficient due diligence or to provide itself with assurances that an illicit payment was unlikely to occur. This aggressive interpretation of the knowledge requirement is contrary to congressional intent in amending the FCPA's knowledge requirement in 1988. *See* Kenneth Winer and Gregory Husisian, "Commentary: The 'Knowledge' Requirement of the FCPA Anti-Bribery Provisions: Effectuating or Frustrating Congressional Intent?", *in* West, White-Collar Crime (Andrews Litigation Reporter), Vol. 24, Issue 1, at 3 (Oct. 2009). Nonetheless, whether in accord with the statute or not, prudence requires that companies adhere to the strict standard that the regulators are likely to apply.

While the nature of the review may vary, depending on the identity of the intermediary, the nature of the circumstances, and other facts and circumstances, the following are a number of steps to consider:

- Contacting the country desk at the State Department, the commercial attaché at the U.S. embassy in the foreign country, and that country's business desk at the Department of Commerce, and asking whether they have any records of improper conduct by the agent or distributor.
- Conducting a basic background check using Dunn & Bradstreet or consult the U.S. Department of Commerce Commercial Service.
- Contacting any references provided to make sure that they actually exist and are willing to vouch for the character of your agent or distributor.
- Checking local databases and/or police records to help determine if the person has a history of being involved in illegal or improper activities (if such resources are not available, local investigatory agencies may serve the same function).
- Establishing written procedures governing how to hire sales agents or distributors.

The goal of such procedures is to take all reasonable steps to check that agents do not appear likely to violate the FCPA and to isolate the actions of a "rogue" agent or distributor if it turns out that it is engaged in FCPA-illegal activity.

The level of inquiry required before hiring a sales agent or distributor will, of course, vary depending upon the facts, the presence of any red flags, and the degree of authority to be granted to the agent or distributor. Lower-level agents are of less concern to the home office; they can be hired and managed by local officials, subject to defined procedures written by the home office. But if the agent will be a key player, or have anticipated government contact, then the U.S. firm should consider exercising greater control.

In deciding which entities to subject to due diligence, companies should keep in mind recent enforcement activity of the U.S. government. Actions of both freight forwarders and Customs brokers have resulted in FCPA enforcement activity, and the U.S. government is likely to scrutinize arrangements that covered persons make with these companies. So, too, are foreign lobbyists a potential FCPA risk, given their frequent contact with foreign legislators. The trend is for companies to subject all of these entities, as well as traditional agents, to due diligence and to treat them as a potential FCPA risk.

One key due diligence goal is to establish that the agent is being properly compensated given the level of responsibility and work required. Doing so serves more than just the business purpose of not overpaying for services rendered, for a payment that is far in excess of what should be required suggests the possibility that the agent is dividing up the proceeds from the arrangement with a government official. A common way to evaluate the reasonableness of compensation is to construct a set of benchmarks within the country at issue, or in countries that are otherwise comparable, for similar work. Of course, this approach works better where the agent is performing relatively simple, often-hired tasks. Nonetheless, the approach does provide some guidance for complicated transactions even if the company cannot determine the exact level of "comparable" work.

Given the importance of due diligence, it is surprising how often firms are haphazard with the results of their due diligence. Companies should not just gather due diligence; they should analyze and summarize it. An adequate summary would note both the positive and negative information gathered and state with particularity how each negative element was handled. It is best if companies keep all information gathered for at least five years after the relationship with the agent or distributor at issue has been terminated.

Written FCPA Procedures. Once a potential agent or distributor has been identified, many companies will request a signed, written questionnaire providing basic information, including: (1) the nature of the agent's or distributor's organization, when and where it was incorporated or registered to do business, and the names of all principals in the organization; (2) a statement that there are no government officials who own or are paid by the intermediary or, if there are, a full disclosure of their names and positions; (3) a copy of the agent's or distributor's most recent fiscal report; (4) a statement regarding whether any of the principals or employees are seeking political office; and (5) a statement regarding prior government positions held by the agent or distributor, or employees of same.

An additional topic, often overlooked, is how far to go in seeking control over subcontractors. The general approach of most companies is to leave the hiring of subcontractors to their agents or joint venture partners. While this can be an attractive proposition from a management standpoint—part of the reason an agent or a joint venture exists, after all, is to introduce this kind of decision-making authority by a knowledgeable local actor into the business relationship—it also can be a risky approach from an FCPA standpoint. Regulators might look at such arrangements, if they have resulted in an illegal payment, with a skewed eye, and to attribute the sins of the subcontractor back to the original hiring entity if there is any evidence of knowledge at all. Therefore, the better approach is to weigh all the factors that raise potential red flags and to set up vetting procedures, especially in countries or industries where problems are likely, and to get involved in the decision to hire subcontractors.

An additional key step is to use tightly worded contractual provisions to provide additional safeguards against FCPA violations. A company should not pay an agent or distributor until there is a written agreement in place that includes appropriate FCPA provisions. Companies should consider having the agent or distributor acknowledge the requirements of the FCPA, agree to be bound by them, and agree to punishment if a violation is suspected. The following are provisions for firms to consider in intermediary contracts:

- The intermediary is an independent contractor with no authority to commit violations of the FCPA.
- The intermediary is aware of the requirements of the FCPA and agrees not to commit any action that would cause an FCPA violation. It is best if the clause explicitly state that the intermediary agrees not to pass on any bribes to foreign officials and not just reference the Act.
- The intermediary is not an employer, officer, or representative of the foreign government, nor a candidate for office. Companies will often require that the intermediary warrant that it will not run for office without first notifying the U.S. firm and allowing it to take appropriate steps in light of this change in status.
- The intermediary will not assign its rights or duties under the agreement without prior written consent of the U.S. corporation.
- The intermediary agrees to allow the issuer's accounting firm to review the intermediary's books.
- The intermediary will conduct all purchases pursuant to an itemized list of expenses and in writing. All reimbursements will occur pursuant to check or wire transfer, never in cash.
- The intermediary agrees that certain expenses, including gifts to any government official exceeding $100, or expenses over a certain amount, will be paid by the intermediary only after it gets approval from the U.S. corporation.
- The intermediary will keep accurate books that show the expenses, the person to whom any payment was made, and a detailed and accurate description of the services, with the company having the right to audit the intermediary's books to satisfy itself that no payment has occurred.
- The U.S. company will be excused from performance or payment if it has any reason to believe that there is any violation of either the U.S. or the foreign company's anti-bribery laws, with the agreement becoming void ab initio.[6]
- The intermediary will notify the U.S. firm if there are any relevant changes in facts, such as a member of the firm becoming a government official.

In addition, the best procedure is for agents and distributors to provide annual

[6] It has become very common for third-party agreements to contain these kinds of void ab initio clauses, or to contain requirements that all funds ever paid under the agreement will be returned if an FCPA violation is uncovered. The DOJ has cited this as a favorable factor in Releases. *See*, *e.g.*, DOJ Releases 94-1 (May 13, 1994) and 08-01 (Jan. 15, 2008).

certifications that they are aware of the requirements of the FCPA, have not made any improper payments, and promise that they will not do so. Annual certifications have the advantage of providing a regular mechanism to capture new hires and also provide ongoing protections should the agent go off the rails and make a payment in violation of the FCPA.

CONCLUSION

Although there is only one FCPA, there is no one correct approach for creating and implementing an FCPA compliance program. The DOJ and the SEC expect that companies will give a great deal of thought to the best way to implement the FCPA's requirements in light of the particular circumstances and the industry involved. Even for companies that regularly are required to operate in environments where requests for bribes are common, there are procedures that companies can put in place to assess and manage the risk of an illicit payment. The use of a systematic, long-term compliance program that is faithfully executed will help ensure that the next time the DOJ or SEC announces an FCPA settlement, it will be with another company.

Author

Gregory Husisian
Of Counsel
Foley & Lardner LLP
202.945.6149
ghusisian@foley.com

APPENDIX: FCPA "RED FLAGS"

General Red Flags

The following are general "environmental" red flags that do not, in and of themselves, indicate specific liability risks with respect to a particular transaction but nonetheless indicate the need for heightened vigilance in general.

Flag 1: Your company has received an "improper payment" audit in the past five years.

Flag 2: Payment in a country with widespread corruption and/or history of FCPA violations occurring in that country. Countries that are considered to fit this category include some Middle Eastern and Asian countries, and much of the former Soviet Union and Africa.

Flag 3: Widespread news accounts of payoffs, bribes, or kickbacks.

Flag 4: The industry involved has a history of FCPA violations. These industries include defense, aircraft, energy, and construction services.

Transaction-Specific Red Flags for Intermediaries

Flag 5: An agent, distributor, or joint venture partner refuses to provide confirmation of willingness to abide by the FCPA.

Flag 6: Family or business ties of an intermediary with a government official.

Flag 7: Bad reputation of the agent or rumors of prior improper payments or other unethical business practices by the intermediary. This is a key flag, and parties should document the good reputation and experience of the intermediaries they hire.

Flag 8: Listing of agent on databases listing known corruption risks like the World Bank List of Debarred Firms.

Flag 9: The intermediary requires that its identity not be disclosed.

Flag 10: The potential foreign government customer recommends the intermediary. This could suggest a coordinated scheme to divide a payoff.

Flag 11: The intermediary lacks the facilities and staff to perform the required services. This could suggest that the intermediary may be performing its job through corrupt payments rather than hard work.

Flag 12: The intermediary is new to the business.

©2010 Gregory Husisian, of Foley & Lardner LLP

Flag 13: The intermediary does not have much experience in the particular industry at issue.

Flag 14: The intermediary has violated local law, even if the violation is not related to bribery.

Flag 15: The intermediary wishes to use anonymous subcontractors.

Flag 16: Unusually large or frequent political contributions to a person or political party by the intermediary, which could suggest an arrangement for the direction of business to the intermediary.

Flag 17: Insistence on the involvement of third parties who appear to be unnecessary for the work required.

Flag 18: A proposed foreign partner is owned by a key government official or a close relative.

Flag 19: Rumors of a silent partner in a joint venture partner, distributor, or agent that is not disclosed by the intermediary.

Flag 20: An intermediary insists on having sole control over meetings with or approvals by a foreign government or government official.

Flag 21: The intermediary has an opaque structure or refuses to reveal the structure.

Flag 22: The intermediary reportedly is associated with criminals or criminal activity.

Flag 23: The proposed relationship is not in accordance with local laws or regulations, including rules dictating when a government official can be involved in a business relationship.

Flag 24: The intermediary attempts to assign its rights or obligations to another party.

Flag 25: The intermediary has an unexplained breakup with another company, which could suggest the discovery of illegal conduct in that relationship.

Flag 26: The intermediary has been investigated for, charged with, or convicted of corruption allegations.

Control-Based Red Flags for Intermediaries

Flag 27: A joint venture partner refuses to agree to reasonable financial controls.

Flag 28: A joint venture partner values assets contributed to the joint venture at an improper value.

Flag 29: A joint venture partner insists on maintaining two sets of books for tax or other purposes.

Flag 30: An intermediary refuses to allow auditing of its books.

Flag 31: An intermediary requests payment of inadequately documented or entirely undocumented expenses.

Flag 32: Any other odd request by an intermediary that reasonably arouses suspicion. For example, if an agent asks that certain invoices he backdated or altered, further inquiry is warranted.

Payment Requests by Intermediaries

Flag 33: Payment of a commission that is at a level substantially above the going rate for agency work in a particular country. An excessive commission might suggest that a portion of the funds is going to a foreign official. Then again, your agent might just be greedy.

Flag 34: Requests to work on contingency or bonus basis. Although such arrangements can be perfectly legitimate, they often are associated with suspicious activity.

Flag 35: Payment through convoluted means. If your agent asks for payment to a numbered account in the Bahamas, the DOJ or SEC could consider this failure to investigate culpable conduct under the FCPA.

Flag 36: Over-invoicing (i.e., the intermediary asks you to cut a check for more than the actual amount of expenses).

Flag 37: Requests that checks be made out to “cash” or “bearer,” that payments be made in cash, or that bills be paid in some other anonymous form.

Flag 38: Requests that payments be made to a third party.

Flag 39: Payment in a third country, which suggests a plan to divide the commission in the third country away from government scrutiny.

Flag 40: Agent or distributor requests for an unusually large credit line for a customer can be suspicious, especially if the customer is new.

Flag 41: Requests for unusual bonuses, one-time success fees, or extraordinary payments.

Flag 42: Requests for an unorthodox or substantial up front payment.

Flag 43: Requests for an increased level of compensation to the intermediary, without a commensurate increase in the amount of work to be performed.

Flag 44: Unexpected requests for reimbursement of entertainment expenses relating to foreign officials.

Flag 45: Any unusual payment requests, such as asking that invoices be backdated or altered.

©2010 Gregory Husisian, of Foley & Lardner LLP